An Enhanced Context Graph Based Framework to Provide a Reliable Strategy for Enhancing Network Security

Reshma Ashik Chauhan

Senior Research Analyst, SMRVD Security Solutions, India.

Abstract: A common firmware makes it easier to control and manage various IoT devices without many overheads. Common software platforms allow easy configurations as well as easy diagnosis of faulty operations. However, a common firmware also subjects the IoT components to various types of threats which can infiltrate the operational defense of these devices. Some of the key features required by IoT networks are remote diagnosis and management, data analytic, software upgrades, information passing and processing, and user mobility identification. All these form a type of application which allows access to the entire network once a particular feature is exploited. In this, a study is presented on the threats for IoT networks and a context graph based framework is presented to provide a strategy for mitigating these attacks.

Keywords: Common firmware, Network Security, Reliability.

1. Introduction

The opportunities for malicious individuals and groups to attempt to gain access to vehicle systems and information could widen significantly if suitable counter-measures are not implemented. Roadside infrastructure and intelligent transport systems (ITS), which are expected to be integrated with vehicle networks via V2X communications, are also potential targets for attack. Furthermore, a modified vehicle could become a 'weapon' for the attacker, by transmitting false warnings and messages in order to subvert the operation of vehicle networks, ITS and telematics services. Ensuring adequate security against such threats will therefore be critical for the successful deployment of V2X and ITS technologies.

The communication networks are observing a tremendous increase in the number of devices which are predicted to go beyond 40% (of that were active in 2012) by 2020. All these devices have been arranged under a common term of "Internet of Things" (IoT). IoT allows integration of the vast variety of communication devices irrespective of their operational technology, which is also a challenging issue as a common firmware is required for all the devices.

Since there is no formal definition of IoT, same attacks which are applicable to any computing entity hold true in their case. Also, reduction in the human interventions and use of more automated systems in the IoT networks make it extremely important to secure the entire network as it may reveal critical information [1-12]. Apart from these, IoT networks are also considered as an integral part of civilian and military expeditions focusing surveillance, navigation, localization, equipment control, and currency transfers, etc.

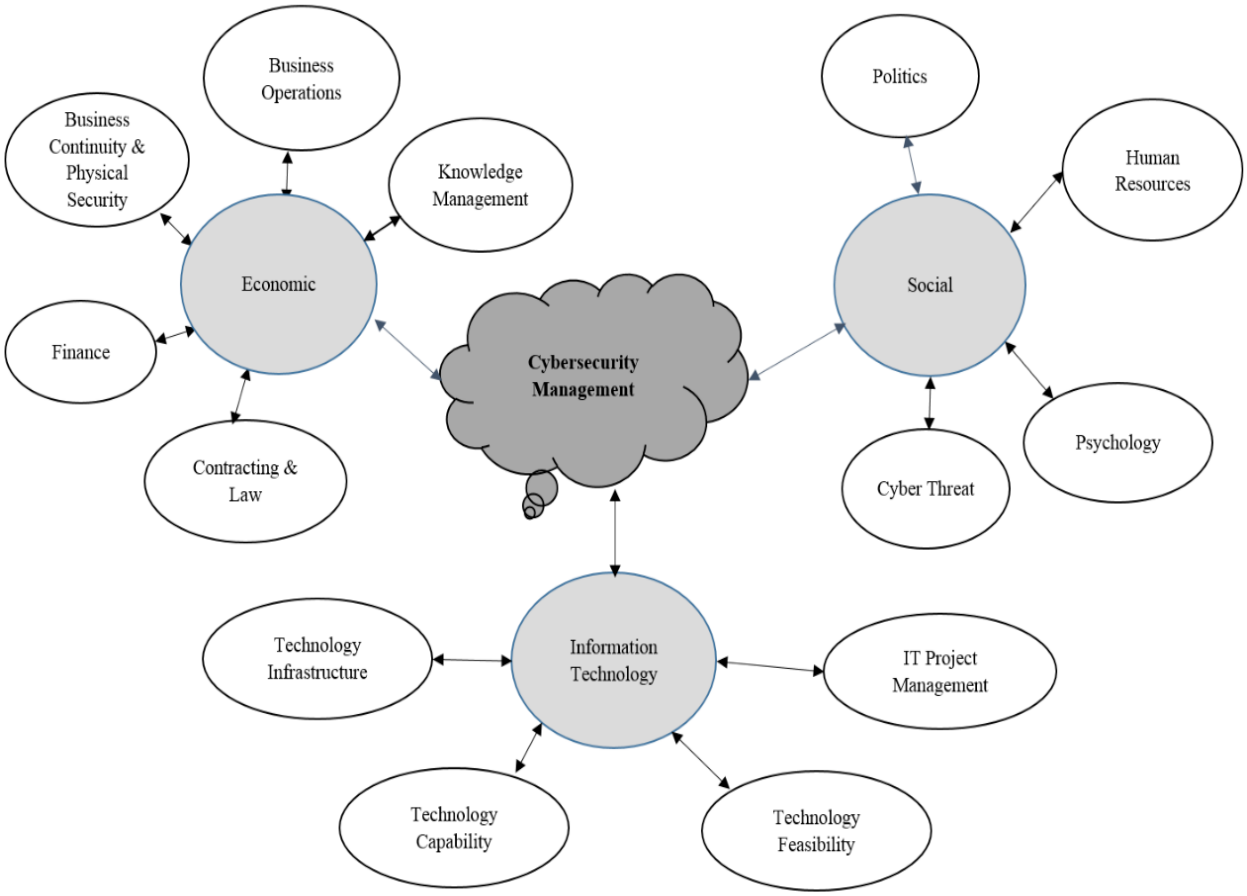

Fig. 1: Cybersecurity Management

Recent trends have focused on using RFID tags as embedded sources for IoT devices that do not connect to the network directly. Although, such strategy holds safe for the majority of application scenarios, but manipulation with RFID tags can easily make these vulnerable similar to a normal computing entity [13-27]. Thus, security of IoT devices irrespective of the mode and type of connectivity is of utmost importance and has been an area of concern for a majority of the security researchers across the globe. Considering a common platform for IoT devices, most of the business enterprises and vendors focus on making version-based IoT firmware that can be easily upgraded and

controlled. Such scenarios are possible by using a software-assisted networking. However, a software-assisted networking suffers from a major issue of zero-day vulnerabilities. Considering the level of deployment and configuration of networks, zero-day vulnerabilities are extremely dangerous for IoT networks [28-39]. Exploitation of a zero-day vulnerability can lead to a zero-day attack. Control over a single unit of IoT software may expose the entire architecture.

The name "Zero-day" is coined considering the negligible time available in mitigating these threats. The number of days for which an anomaly has been known directly affects the countermeasures and also the probability of remaining affected. It also has to do a lot with those software users who do not update security patches regularly [40-51]. Once a vulnerability is publicized, it is mandatory for the particular application users to immediately switch to the stable releases. However, failure in doing so leads to various consequences in the form of cyber-attacks.

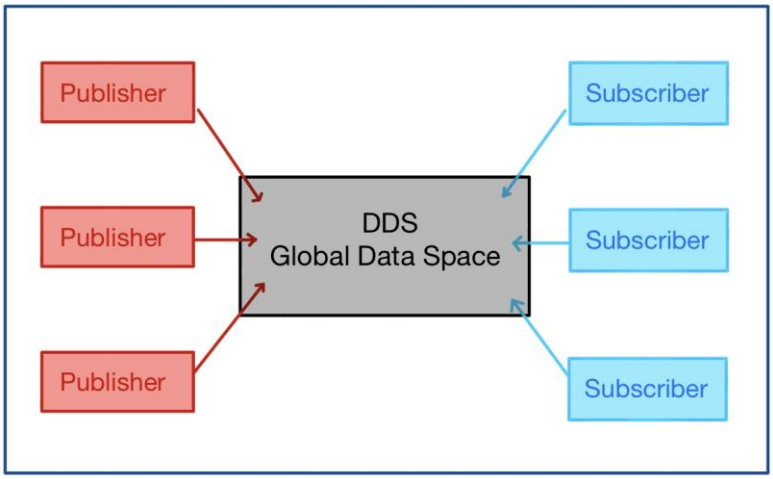

Fig. 2: DDS Based Coding

The effect of a zero-day vulnerability also depends on the mode of detection. If a vulnerability is identified by white hat hackers, it allows keeping it low profile until the security patches are not available; whereas identification of such vulnerabilities by a notorious group (black hat hackers) may subject the entire enterprise to failure. The vulnerability cycle for a zero-day attack may vary from scenario to scenario. In some cases, after identification of a bug, the hackers operate covertly leading to the full zero-day attack, while in some cases, the hackers may come forward (overt) and make threat public. Thus, it can be analyzed that a zero-day attack is not only because of the covert behavior of a hacker but also because of the delays in updating security patches once these are available in the public domain.

This is often explained in the terms of window of vulnerability. The window of vulnerability is the time gap in which the number of vulnerable systems remaining is negligible. It is evaluated as a software timeline considering the discovery phase, security patching, intermediate exploitation phase and patch applicability phase.

For safety-related control systems, of which vehicles are perhaps the most widely encountered examples, it is possible that some cyber security threats may also have safety implications [52-64]. This possibility is now reflected in IEC 61508, the functional safety standard for safety-related electronic control systems in the process industries. However, security threats that are not safety-related, such as those affecting privacy or financial security, are beyond the scope of IEC 61508.

Standards and guidelines have already been developed to help ensure the security of information technology (IT) systems. However, as some cyber security threats to cyber physical systems may also impact on functional safety, there is a need to ensure that their treatment meets the requirements of safety engineering processes. Standards and guidelines have already been developed for functional safety of safety-related control systems, including vehicles.

There is also a need to adapt IT security evaluation approaches in order to address the particular issues of automotive applications, such as the possibility that a security threat may also have safety implications. This section therefore summarizes a number of key concepts from these two disciplines.

2. Methodology

The network comprises various IoT devices and gadgets that operate either individually or collectively via a common gateway. The communication can be directly between the Mobile Node (MN) and the IoT device or indirectly between the MN and the IoT device via a gateway. The service providers are responsible for maintaining trust between the IoT and the MN.

Currently, the proposed model emphasizes on a particular scenario in which an IoT device receives security updates that may lead to zero-day attacks; or when an attack is already launched and security updates confirm the attacks. The proposed approach uses strategic context graphs to ensure the safety of IoT devices against the zero-day attacks. The context graphs are implemented using Distributed Diagnosis System (DDS). The DDS are divided into three parts:

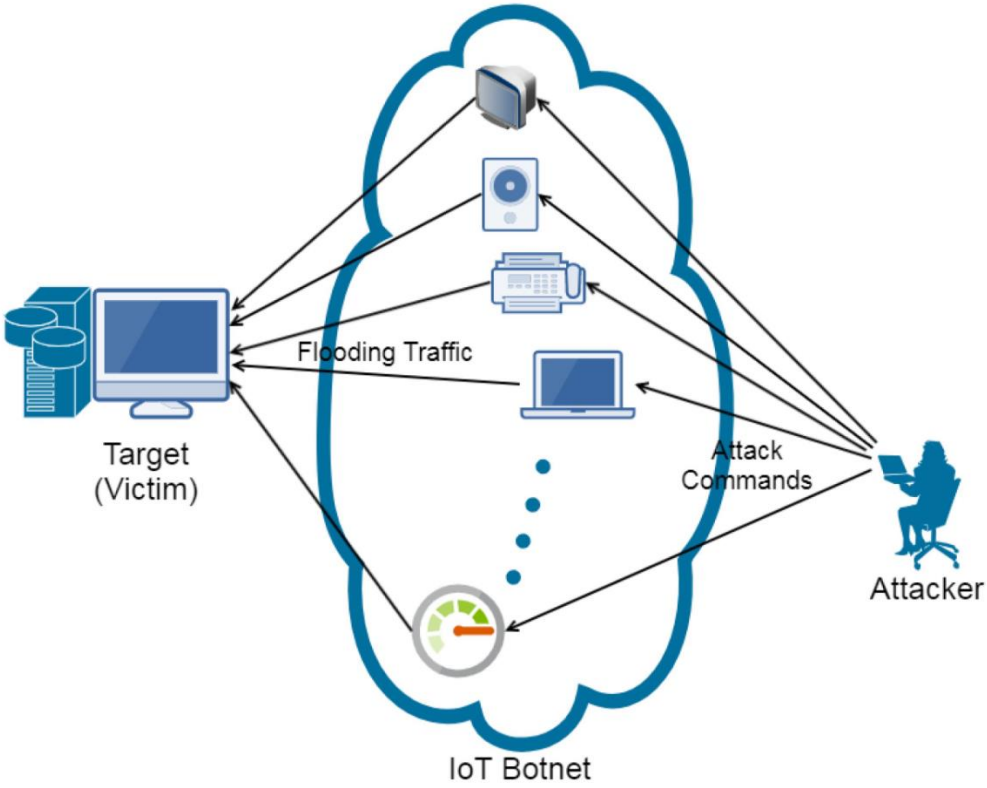

Fig. 3: An illustration of attacks

(1) Central Diagnosis System (CDS): CDS is installed by the service providers on the central node of the network which is responsible for generating trust as well as the updates for the entire network. CDS is responsible for managing the Access Points (APs) control, and the operations of gateways for maintaining security in the case of high possibilities of threats.

(2) Local Diagnosis System (LDS): LDS is operated as a dedicated device over the gateways. Usually, these are installed with the Home Gateways (HGW). LDS interacts with the CDS and shares its context graphs with it to ensure that all the security procedures are followed by the corresponding IoT device.

(3) Semi Diagnosis System (SDS): SDS is responsible for directly managing the APs trust with the CDS. It shares the context of IoT devices which directly interacts with an MN without relying on the local gateway.

3. Strategic Context

Device signatures (S_g): This is the unique identity for each device. The signature is the embedded information about the IoT device which is stored at the CDS once it gets activated in the network.

Update Counter (U_c): This is the firmware update counter which is randomly selected at the beginning of network registrations. These are updated using random integer values which are finalized by the CDS and change periodically without affecting the performance.

Traffic Type (T_p): This defines the context for the type of traffic to be generated for and by an IoT device. This helps the diagnosis system to analyze the content over a particular channel for its correctness.

Header Length (H_l): It defines the bit length of the header field used by the diagnosis system. It contains all the necessary context metadata which is to be shared between the LDS, SDS, and CDS.

Memory Range (M_r): It denotes the maximum and minimum size of the packets generated by the IoT device. This helps to simply analyze if the size of the initial code is affected or not. Usually, these are not mishandled by the attackers, but still, in some cases, this is very useful to identify if the binaries of the firmware are altered or not.

The types of devices operable in a network are considered to have valid pre-registered signatures along with a counter value. The counter value manages the count for the number of times the firmware of an IoT device is validated or encountered. The context for each IoT device is managed by its diagnosis system and periodically stored in logs and shared with the CDS. The context outline used in the proposed model is as follows:

Route (R_t): This field is used to check whether an IoT device is operable in LDS, SDS, or CDS region. This also allows tracking the actual route for managing the context between the network entities.

The context graphs are used to generate the strategies which help in taking a decision regarding the presence of a threat amongst the IoT devices. The number of vertices in the context graphs is equal to the number of processing procedures an IoT device follows before generating an output and demanding an input. The context explained above forms the edges of the graph. After the time instance decided in the configuration of the network, the LDS and SDS evaluate these graphs for every corresponding IoT device ad share it with the CDS which also forms its own context graph for every IoT device. Along with the context graphs, the CDS also forms the context graphs for the subordinate network which includes the layers of APs, and gateways.

In order to take a strategic decision on the management of IoT devices against the zero-day attacks, the CDS follows a principle of modeling the counter and the random integer value used to manage the counter by the LDS, SDS and the device itself. Then, it performs mutual exclusion rule to trace the presence of a zero-day threat in the IoT network. The failure in the matching of the context stored and the context received from all the subordinates as well as the IoT device indicates the presence of a zero-day attack.

It is to be noted that the strategic context graphs are applicable in the network only in the deployment phase, but not in the development phase. Thus, the proposed strategy can come handy only when a vulnerability is identified by the development team at lateral stages as well as during the release of security updates as it helps in tracking the contextual behavior of every IoT device. Once a possibility of attack is found, the proposed approach utilizes the critical data sharing protocol that helps in eliminating a particular IoT device before it exploits the entire network.

The proposed approach uses a critical context/data sharing protocol in the scenarios with a potential zero-day threat. The protocol illustrates the procedures opted by the CDS once a threat is identified amongst the IoT devices leading to a zero-day exploitation. Once a threat policy is violated, the CDS sends alarming messages to its connected components that are its subordinates in the network. The alarming messages are followed by the patch for fixing the affected IoT device. This is followed by the reestablishment of the trust between all the connected components with the CDS. Once an alarming request is received, each subordinate's diagnosis system shares context information to revalidate the trust. By the time, these steps are performed, the affected device updates its security mechanisms, and registers itself again with the CDS leading to the elimination of the threat without eliminating the device. On the contrary, CDS shares threat information with the SDS, trust information with the HGW, device information with the LDS, and finally, leads it to eliminate the incorrect device. This allows mitigating zero-day threats in IoT networks.

4. Conclusions

The proposed approach used a distributed diagnosis system for classifying the context at the central service provider as well as at the local user site. Also, once a zero-day attack was potentially identified, a critical data sharing protocol was used to transmit alert messages and reestablish the trust between the network entities and the IoT devices. This is a progressive paper and the details on the full-fledged implementation along with critical evaluations will be presented in future reports.

References

[1] G. Goggin, ―Driving the internet: Mobile internets, cars, and the social, Future Internet, 2012.

[2] G. Qian, Y. Wu, and Q. Shao, ―A procedure for estimating the number of clusters in logistic regression clustering, J. Classification, vol. 26,no. 2,pp. 183–199, 2009.

[3] H. Panetto and J. Cecil, ―Information systems for enterprise integration, interoperability and networking: Theory and applications, Enterprise Inf. Syst., vol. 7, no. 1, pp. 1–6, 2013.

[4] H. Wang, W. He, and F. K. Wang, ―Enterprise cloud service architectures, Inf. Technol. Manag., vol. 13, no. 4, pp. 445–454, 2012.

[5] H. Abid, L.T.T. Phuong, J. Wang, S. Lee, and S. Qaisar,―V-Cloud: Vehicular cyber-physical systems and cloud computing, in Proc. 4th Int. Symp. Appl. Sci. Biomed. Commun. Technol., Barcelona, Spain, 2011, p. 165.

[6] Vinod Varma Vegesna (2023). "Adopting a Conceptual Architecture to Mitigate an IoT Zero-Day Threat that Might Result in a Zero-Day Attack with Regard to Operational Costs and Communication Overheads," International Journal of Current Engineering and Scientific Research, Volume-10, Issue-1, Pages 9-17.

[7] Vinod Varma Vegesna (2023). "Methodology for Mitigating the Security Issues and Challenges in the Internet of Things (IoT) Framework for Enhanced Security," Asian Journal of Basic Science & Research, Vol. 5, No. 1, January-March 2023, Pages 85–102, doi: 10.38177/ajbsr.2023.5110.

[8] Hamid Ali Abed Al-Asadi, et al., "Nature Inspired Algorithms multi-objective histogram equalization for Grey image enhancement", Advances in Computer, Signals and Systems (2020) 4: 36-46 Clausius Scientific Press, Canada DOI: 10.23977/acss.2020.040106.

[9] Hamid Ali Abed Al-Asadi and et al., " Critical Comparative Review of Nature-Inspired Optimization Algorithms (NIOAs), International Journal of Simulation: Systems, Science and Technology (IJSSST), 2020, 21(3), PP1-15

[10] Hamid Ali Abed Al-Asadi, (2022) "1st Edition: Privacy and Security Challenges in Cloud Computing A Holistic Approach" Intelligent Internet of Things for Smart Healthcare Systems, Scopus, Taylor @Francis, CRC Press. (Book Chapter: Enhanced Hybrid and Highly Secure Cryptosystem for Mitigating Security Issues in Cloud Environments), March 2022.

[11] Vinod Varma Vegesna (2023). "Secure and Reliable Designs for Intrusion Detection Methods Developed Utilizing Artificial Intelligence Approaches," International Journal of Current Engineering and Scientific Research, Volume-10, Issue-3, Pages 1-7.

[12] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, ―Internet of things(IoT): A vision, architectural elements, and future directions, Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.

[13] J. Wang, J. Cho, S. Lee, and T. Ma, ―Real time services for future cloud computing enabled vehicle networks, in Proc. Int. Conf. Wireless Commun. Signal Process., Nanjing, China, 2011.

[14] Vinod Varma Vegesna (2023). "A Critical Investigation and Analysis of Strategic Techniques Before Approving Cloud Computing Service Frameworks," International Journal of Management, Technology and Engineering, Volume XIII, Issue IV, April 2023, Pages 132-144.

[15] Vinod Varma Vegesna (2023). "A Comprehensive Investigation of Privacy Concerns in the Context of Cloud Computing Using Self-Service Paradigms," International Journal of Management, Technology and Engineering, Volume XIII, Issue VII, July 2023, Pages 173-187.

[16] L. Atzori, A. Iera, and G. Morabito, ―The internet of things: A survey, Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.

[17] C. Speed and D. Shingleton, ―An internet of cars: Connecting the flow of things to people, artefacts, environments and businesses, in Proc.6thACM Workshop Next Gener. Mobile Comput. Dynam. Personalised Travel Plann. ACM, Ambleside, U.K., 2012, pp. 11–12.

[18] D. Lowd and P. Domingos, ―Naive Bayes models for probability estimation, in Proc. 22nd Int. Conf. Mach. Learn., Bonn, Germany: ACM, 2005, pp. 529–536.

[19] D. Paulraj, S. Swamynathan, and M. Madhaiyan, ―Process model-based atomic service discovery and composition of composite semantic web services using web ontology language for services (OWL-S), Enterprise Inf. Syst., vol. 6, no. 4, pp. 445–471, 2012.

[20] Vinod Varma Vegesna (2022). "Using Distributed Ledger Based Blockchain Technological Advances to Address IoT Safety and Confidentiality Issues," International Journal of Current Engineering and Scientific Research, Volume-9, Issue-3, Pages 89-98.

[21] Vinod Varma Vegesna (2022). "Methodologies for Enhancing Data Integrity and Security in Distributed Cloud Computing with Techniques to Implement Security Solutions," Asian Journal of Applied Science and Technology, Volume 6, Issue 2, Pages 167-180, April-June 2022, doi: 10.38177/ajast.2022.6217.

[22] Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, Hamzah F. Zmezm, Dr. Hussain Falih Mahdi, Hassan Muhsen Abdulkareem Al-Haidari. "Suggested Mechanisms for Understanding

the Ideas in Authentication System," International Journal of Advancements in Computing Technology9(3):10-24, 2018.

[23] Hamid Ali Abed Al-Asadi and et al., "Priority Incorporated Zone Based Distributed Clustering Algorithm For Heterogeneous Wireless Sensor Network", Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 5, PP. 306-313, 2019.

[24] Hamid Ali Abed Al-Asadi and et al., "A Network Analysis for Finding the Shortest Path in Hospital Information System with GIS and GPS, Journal of Network Computing and Applications (2020) 5: 10-22.

[25] Vinod Varma Vegesna (2022). "Utilising VAPT Technologies (Vulnerability Assessment & Penetration Testing) as a Method for Actively Preventing Cyberattacks," International Journal of Management, Technology and Engineering, Volume XII, Issue VII, July 2022, Pages 81-94.

[26] Vinod Varma Vegesna (2022). "Accelerate the development of a business without losing privacy with the help of API Security Best Practises - Enabling businesses to create more dynamic applications," International Journal of Management, Technology and Engineering, Volume XII, Issue IX, September 2022, Pages 91-99.

[27] E. Qin, Y. Long, C. Zhang, and L. Huang, ―Cloud computing and the internet of things: Technology innovation in automobile service, in Human Interface and the Management of Information. Information and Interaction for Health, Safety, Mobility and Complex Environments. Berlin, Germany: Springer-Verlag, 2013, pp. 173–180.

[28] F. Tao, H. Guo, L. Zhang, and Y. Cheng, ―Modelling of combinable relationship-based composition service network and the theoretical proof of its scale-free characteristics, Enterprise Inf. Syst., vol. 6, no. 4,pp. 373–404, 2012.

[29] W. Lumpkins, ―The internet of things meets cloud computing, IEEE Consum. Electron. Mag., vol. 2, no. 2, pp. 47–51, Apr. 2013.

[30] Y. Leng and L. Zhao, ―Novel design of intelligent internet-of-vehicles management system based on cloud-computing and internet of-things, in Proc. Int. Conf. Electron. Mech. Eng. Inf. Technol., Harbin, Heilongjiang, China, 2011, vol. 6, pp. 3190–3193.

[31] Vinod Varma Vegesna (2022). "Investigations on Cybersecurity Challenges and Mitigation Strategies in Intelligent transport systems," Irish Interdisciplinary Journal of Science and Research, Vol. 6, Iss. 4, Pages 70-86, October-December 2022, doi: 10.46759/iijsr.2022.6409.

[32] Vinod Varma Vegesna (2021). “Analysis of Data Confidentiality Methods in Cloud Computing for Attaining Enhanced Security in Cloud Storage,” Middle East Journal of Applied Science & Technology, Vol. 4, Iss. 2, Pages 163-178, April-June 2021, Available at SSRN: https://ssrn.com/abstract=4418127

[33] Hamid Ali Abed Al-Asadi and Majda Ali Abed, "Object Recognition Using Artificial Fish Swarm Algorithm on Fourier Descriptors," American Journal of Engineering, Technology and Society; Volume 2, Issue 5: pp. 105-110, 2015.

[34] Hamzah F. Zmezm, Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, "A Novel Scan2Pass Architecture for Enhancing Security towards E-Commerce," Future Technologies Conference 2017, 29-30 November 2017 | Vancouver, BC, Canada, 2017.

[35] Hamid Ali Abed Al-Asadi, Majida Ali Al-Asadi, Nada Ali Noori , "Optimization Noise Figure of Fiber Raman Amplifier based on Bat Algorithm in Optical Communication network," International Journal of Engineering & Technology, Scopus, Vol 7, No 2, pp. 874-879, 2018.

[36] Vinod Varma Vegesna (2021). “A Highly Efficient and Secure Procedure for Protecting Privacy in Cloud Data Storage Environments,” International Journal of Management, Technology and Engineering, Volume XI, Issue VII, July 2021, Pages 277-287.

[37] Vinod Varma Vegesna (2021). “The Utilization of Information Systems for Supply Chain Management for Multicomponent Productivity Based on Cloud Computing,” International Journal of Management, Technology and Engineering, Volume XI, Issue IX, September 2021, Pages 98-113.

[38] Y. Li, M. Hou, H. Liu, and Y. Liu, ―Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of internet of things, Inf. Technol. Manag., vol. 13, no. 4, pp. 205–216, 2012.

[39] Y. Qin, D. Huang, and X. Zhang, ―VehiCloud: Cloud computing facilitating routing in vehicular networks, in Proc. IEEE 11th Int. Conf. Trust Secur. Privacy Comput. Commun., Liverpool, U.K., 2012,pp. 1438–1445.

[40] Y. Zhang, B. Chen, and X. Lu, ―Intelligent monitoring system on refrigerator trucks based on the internet of things, Wireless Communications and Applications. Berlin, Germany: Springer-Verlag, 2012, pp. 201–206.

[41] Vinod Varma Vegesna (2021). “The Applicability of Various Cyber Security Services for the Prevention of Attacks on Smart Homes,” International Journal of Current Engineering and Scientific Research, Volume-8, Issue-12, Pages 14-21.

[42] Vinod Varma Vegesna (2020). “Secure and Privacy-Based Data Sharing Approaches in Cloud Computing for Healthcare Applications,” Mediterranean Journal of Basic and Applied Sciences, Volume 4, Issue 4, Pages 194-209, October-December 2020, doi: 10.46382/mjbas.2020.4409.

[43] Majida Al-Asadi, Yousif A. Al-Asadi, Hamid Ali Abed Al-Asadi, "Architectural Analysis of Multi-Agents Educational Model in Web-Learning Environments," Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 6, 2012.

[44] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "Simplifying Handwritten Characters Recognition Using a Particle Swarm Optimization Approach”, European Academic Research, Vol 1,pp. 535- 552, Issue(5), 5. 2013.

[45] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "High Accuracy Arabic Handwritten Characters Recognition using (EBPANN) Architecture," International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 6 Issue 2, 2015.

[46] Vinod Varma Vegesna (2019). “Investigations on Different Security Techniques for Data Protection in Cloud Computing using Cryptography Schemes”, Indo-Iranian Journal of Scientific Research, Volume 3, Issue 1, Pages 69-84, January-March 2019, Available at SSRN: https://ssrn.com/abstract=4418119

[47] Z. Pang, L. Zheng, J. Tian, S. Kao-Walter, E. Dubrova, and Q. Chen,―Design of a terminal solution for integration of in-home health care devices and services towards the internet-of-things, Enterprise Inf. Syst., to be published, 2014.

[48] L. Ren, L. Zhang, F. Tao, X. Zhang, Y. L. Luo, and Y. Zhang,―A methodology towards virtualization-based high performance simulation platform supporting multidisciplinary design of complex products, Enterprise Inf. Syst., vol. 6, no. 3, pp.267–290, 2012.

[49] R. Mietzner, F. Leymann, and T. Unger, ―Horizontal and vertical combination of multi-tenancy patterns in service-oriented application, Enterprise Inf. Syst., vol. 5, no. 1, pp. 59–77, 2011.

[50] S. Bitam and A. Mellouk, ―ITS-cloud: Cloud computing for intelligent transportation system, in Proc. IEEE Global Commun. Conf., Anaheim, CA, USA, 2012, pp. 2054–2059.

[51] S. Hachani, L. Gzara, and H. Verjus, ―A service-oriented approach for flexible process support within enterprises: Application on PLM systems, Enterprise Inf. Syst., vol. 7, no. 1, pp. 79–99, 2013.

[52] S. Li, L. Xu, and X. Wang, ―Compressed sensing signal and data acquisition in wireless sensor networks and internet of things, IEEE Trans. Ind. Informat., vol. 9, no. 4, pp. 2177–2186, Nov. 2013.

[53] Vinod Varma Vegesna (2018). "Analysis of Artificial Intelligence Techniques for Network Intrusion Detection and Intrusion Prevention for Enhanced User Privacy", Asian Journal of Applied Science and Technology, Volume 2, Issue 4, Pages 315-330, Oct-Dec 2018, Available at SSRN: https://ssrn.com/abstract=4418114

[54] Vinod Varma Vegesna (2017). "Incorporating Wireless Sensor Networks and the Internet of Things: A Hierarchical and Security-Based Analysis," International Journal of Current Engineering and Scientific Research, Volume-4, Issue-5, Pages 94-106, Available at SSRN: https://ssrn.com/abstract=4418110

[55] Hamid Ali Abed Al-Asadi, Majida Ali Abed, AL-Asadi, Zainab sabah, Baha Al-Deen, Ahmad Naser Ismail, "Fuzzy Logic approach to Recognition of Isolated Arabic Characters", International Journal of Computer Theory and Engineering, Vol. 2, No. 1, 1793-8201, February, 2010.

[56] H. A. Al-Asadi, M.H. Al-Mansoori, S. Hitam, M. I. Saripan, and M. A. Mahdi, "Particle swarm optimization on threshold exponential gain of stimulated Brillouin scattering in single mode fibers," Optics Express, vol. 19, no. 3, pp. 1842-1853, 2011.

[57] Vinod Varma Vegesna (2016). "Threat and Risk Assessment Techniques and Mitigation Approaches for Enhancing Security in Automotive Domain," International Journal of Management, Technology And Engineering, Volume VI, Issue II, July-Dec 2016, Pages 314-331, Available at SSRN: https://ssrn.com/abstract=4418100

[58] Vinod Varma Vegesna (2015). "Incorporating Data Mining Approaches and Knowledge Discovery Process to Cloud Computing for Maximizing Security," International Journal of Current Engineering and Scientific Research, Volume-2, Issue-6, Pages 118-133, Available at SSRN: https://ssrn.com/abstract=4418107

[59] S. Olariu, I. Khalil, and M. Abuelela, ―Taking VANET to the clouds, Int. J. Pervasive Comput. Commun., vol. 7, no. 1, pp. 7–21, 2011.

[60] L. Xu, ―Enterprise systems: State-of-the-art and future trends, IEEE Trans. Ind. Informat., vol. 7, no. 4, pp. 630–640, Nov. 2011.

[61] P. Jaworski, T. Edwards, J. Moore, and K. Burnham, ―Cloud computing concept for intelligent transportation systems, in Proc. 14th Int. IEEE Conf. Intell. Transp. Syst., 2011, pp. 391–936.

[62] P. Papadimitratos, A. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, ―Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation, IEEE Commun. Mag., vol. 47, no. 11, pp. 84–95, Nov. 2009.

[63] Q. Li, Z. Y. Wang, W. H. Li, J. Li, C. Wang, and R. Y. Du, ―Applications integration in a hybrid cloud computing environment: Modeling and platform, Enterprise Inf. Syst., vol. 7, no. 3, pp. 237–271, 2012.

[64] R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh, ―Rethinking vehicular communications: Merging VANET with cloud computing, in Proc. IEEE 4th Int. Conf. Cloud Comput. Technol. Sci., Taipei, Taiwan, 2012, pp. 606–609.